The Deputy Director of Central Intelligence

Washington D C 20505

25X1 ER 448/84
31 January 1984

MEMORANDUM FOR: See Distribution

SUBJECT: Development of an Intelligence Community Point Paper on Threats to Automated Information Systems

REFERENCE: 28 November 1983 Computer Security (COMPUSEC) Project Seniors' Brief

25X1

25X1 1. During referent briefing, noted that the Intelligence Community needs to develop a threat assessment on computer security. The COMPUSEC project includes a task to identify specific threats to and vulnerabilities in our automated systems.

25X1 2. We have asked Chief of CIA's Information Systems Security Group, to develop a coordinated point paper by 15 February 1984 as an NFIB assessment that can be used to brief appropriate Congressional staffs during their review of the FY 85 NFIP budget.

25X1 3. Please nominate a staff member to support in his
25X1 efforts to develop this assessment. (secure).

25X1

John N. McMahon

Distribution:
1 - D/NSA
1 - D/DIA
1 - D/FBI
1 - ASD(C^3I)
1 - D/INR
1 - ExDir/CIA

* I ASSUME VERBAL DISCUSSIONS PERMIT THIS DEADLINE TO BE REASONABLE

25X1

WARNING NOTICE
INTELLIGENCE SOURCES
OR METHODS INVOLVED

COMPUSEC AND COMSEC THREAT TO AUTOMATED INFORMATION HANDLING SYSTEMS

I. THE ISSUES

° A formulation of the "threat" to automated information handling systems which process and disseminate classified Intelligence information.

° Implementation of actions to reduce significantly the vulnerabilities of existing Intelligence information handling systems.

II. DESCRIBING THE THREAT

The automated Intelligence information handling systems for which the threat is being formulated are depicted in Figure 1. The threat can be considered as being directed against:

A. The computer assets of the system.

B. The communication assets of the systems.

C. The personnel directly associated with system operation.

D. The customers (or users) of the system having access either to system equipment (computer/communications assets) or to system products.

This above listing delineates the targets of the threat.

The sources of the threat can be categorized as any combination of:

A. Domestic Threat (DEFINE)

B. Foreign Threat (DEFINE)

C. Internal Threat (DEFINE)

D. External Threat (DEFINE)

Traditionally, both the targets and the sources of any threat have been qualitatively - as opposed to quantitatively - described.

III. THE TARGET POPULATION

The complete target population is all automated systems handling classified Intelligence information. The specific and limited target population for which the threat will be discussed in this paper is made up of all automated systems handling SCI information. Precise data do not yet exist. The best existing data yields the following target population characteristics:

A. Automated SCI Handling Systems

1. Numbers
2. Location (CONUS, foreign...)

B. Computer Assets

1. Computer Models
2. Operating Systems in Use

C. Communications Networks

1. Numbers
2. - - - -
3. - - - -

D. Personnel Directly Associated with System Operation

E. Customers (or Users)

In addition to these gross population data, other distinguishing characteristics are:

A. System High

B. Interconnectivity

etc.

IV. THREAT CHARACTERISTICS

The threat spectrum is depicted in Figure 2. The extremes of the threat spectrum can be viewed as follows:

- The minimum threat (low end of threat spectrum).

  (Definition in Seniors' Briefing)

- The maximum threat (upper end of threat spectrum).

Threat determination evolves from two principal lines of investigation. A first means of sizing and identifying the threat is through knowledge of system vulnerabilities followed by a priority ranking of these vulnerabilities in terms of ease of exploitation. A second means of sizing and identifying the threat is through the Intelligence processes of :

- Discovering penetrations or successful attacks.
- Traditional - targeting of human resources.
- CI.

Approved For Release 2008/10/07 : CIA-RDP89B01354R000100190002-9